IPv6: KEY TO ARMY FUTURE FORCE NET-CENTRIC CAPABILITIES

T. J. Walsh, Author
US Army PD CHS/Northrop Grumman
Fort Monmouth, NJ 07703

Dr. A. K. Jain, Coauthor
US Army PD CHS
Fort Monmouth, NJ 07703

K.F. Chan, Coauthor
US Army CERDEC
Fort Monmouth, NJ 07703

ABSTRACT

This paper reports on the Next Generation Internet Protocol (IPv6), a key enabler to the achievement of Net-centric capabilities to support the Army's Future Force. In addition, the paper describes the Fort Monmouth IPv6 Center of Excellence initiatives undertaken in response to the difficult IPv6 transitional challenges. It also presents the positive operational results, obtained from participating in the 2006 Joint User Interoperability Communications Exercise (JUICE), that focused on interoperability of IPv6 Transition Mechanisms, automated task force reorganization, and mobility capabilities enabled by IPv6 support for the warfighter.

1. INTRODUCTION

Army Network Centric Future Force

The Army is aggressively planning to transform itself from the current complex legacy force to a significantly more information-powered, seamless Future Force over the next decade. The Future Force will involve the integration of the Future Combat System (FCS), the Objective Force Warrior (OFW), and other Objective Force programs combining with and regenerating the Modular Army of today. A central theme to all these Future Force efforts and legacy systems, that will successfully evolve into the future, is achieving Net-centric operations and warfare capabilities for the Army, by capitalizing on a wide spectrum of advanced technologies. Figure 1 shows some of the network complexity involving platforms and systems of the Army and Joint network-centric Future Force.

The underlying concepts and benefits of Network Centric Warfare (NCW) have been well addressed in the literature <r1, r2>. NCW embodies full use of information technology by the by the Department of Defense (DoD), via shared and collaborative use of information on the battlefield.

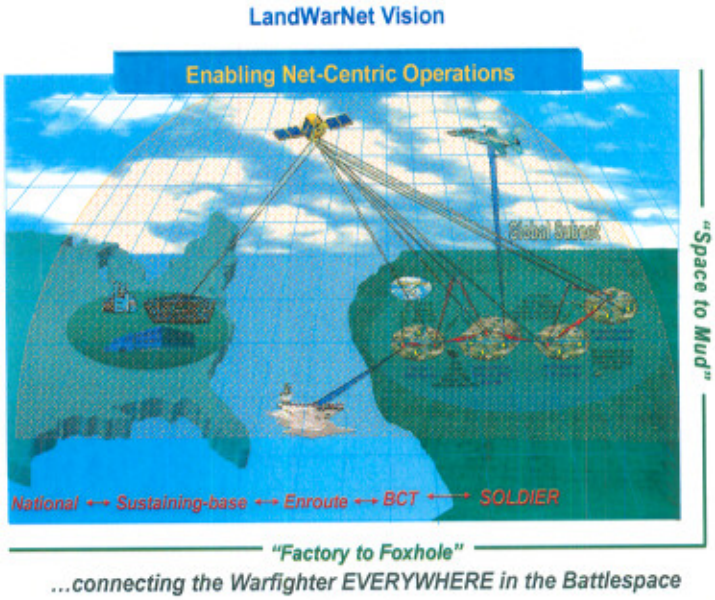


Figure 1

The latest technology for the Future Force includes a range of computer hardware processors, the Next Generation Internet, intelligent agent software, land and air robotics, and a suite of sensors integrated into a unified information network. For the NCW, the network itself and its advanced features is the salient feature of the Future Force architecture.

The Army Future Force envisioned by the DoD, in its transformation process, must posses technological capabilities for the full spectrum of military operations <r3>. One of the most challenging aspects of military operations is achieving information superiority in information collection, processing, distribution, and

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
01 NOV 2006	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
IPv6: Key to Army Future Force Net-Centric Capabilities	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **US Army PD CHS/Northrop Grumman Fort Monmouth, NJ 07703**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADM002075., The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**8**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

communication networks. Future communications networks will have a critical dependency on the rapidly maturing network technology dominated by the Internet Protocol Version 6 (IPv6), and other related network advances such as the NSA High Assurance Internet Protocol Encryption standard and Voice over Internet Protocol (VoIP) <r4> that will augment IPv6 to produce a system of systems architecture.

The remainder of this paper examines the unique Future Force technology challenges from a networking perspective, analyzing emerging networking capabilities against desired operational results. The application of a systematic risk management approach and pragmatic technology initiatives seem a prudent approach to learn, evaluate, integrate and deploy the best technologies and capabilities to the warfighter.

It is becoming widely accepted by the DoD and other organizations that IPv6 technology is an essential key to enabling Net-centric architecture.

2. Internet Protocol Version 6 (IPv6) Technology and Benefits

IPv4 has served the technical community well over the last quarter of century, but has serious limitations and shortcomings for the Army's Future Force networking requirements. These limitations include sheer network complexity, available address space, performance, and security considerations. IPv6 is a suite of protocol standards and specifications that define the next generation Internet Protocol, including advanced network capabilities as described in many technical books and publications <r5,r6>. The Department of Defense has fully endorsed this new standard through policy guidance requiring that all Global Information Grid (GIG) assets be IPv6 capable after 1 October 2003 <r7> and identifying the goal of transitioning by 2008 <r8>. This transition includes the important additional requirement to maintain interoperability with the IPv4 network and devices. The Office of Management Budget has also issued a directive <r9>, in recognition of the technological impacts to the nation and high international economic stakes, that all federal infrastructures must transition their network backbones to IPv6 by June of 2008.

IPv6 is an extensive upgrade to IPv4 and Figure 2 shows key IPv6 features and benefits. Several of the IPv6 features are of particular relevance to the Army and will be further presented here:

- Significantly Increased Address Space
- Simplified Header
- Auto-Configuration
- Improved Mobility Support
- Improved End-to-End Security
- Quality of Service/Flow Labeling
- Multicast and Anycast Distribution

Key IPv6 Features and Benefits

Figure 2

IPv6 header provides 128 bits for addressing, about one third of a duodecillion for address space, combined with more levels of hierarchy. This will offer virtually no restrictions to the continued use of the IPv6, without concern for address exhaustion, and allow easy addition of all types of mobile and static devices. The virtual unlimited address space is important to the Army Future Force, which is expected to employ addressable wearable computers, PDAs, laptops, unmanned sensors, robotics, vehicles loaded with computers, and network devices providing the connected infrastructure.

IPv6 has several features that may reduce packet forwarding overhead. It also has a simplified, fixed-length header and fields that are aligned for 64-bit processors. Hierarchical addressing allows a reduction in the size and complexity of routing tables, allowing for faster packet processing. This increase in the speed of packet processing and simplified overhead should lead to significant performance improvements in overall network traffic flow.

IPv6's stateless auto-configuration capability has been designed to ensure that hosts do not need to be manually configured in an error-prone process that requires highly skilled administrators, before they are connected to the network. This is important to the Army, because less manual work is required when a unit initially deploys or is reorganized in the field. Stateless auto-configuration is new and unique to IPv6. IPv6-based technology has built-in advantages for mobile user devices, ad-hoc networks, and mobile service providers. IPv6 nodes can discover each other and form IPv6

addresses to communicate on a network, using what is called "Neighbor Discovery" and "Stateless Auto-configuration" features. Army users will be able to establish communications in a dynamic battlefield with greater efficiency and robustness than using the IPv4 protocol. In addition, IPv6 defines a protocol for Network Mobility (NEMO) that has powerful network implications for the Army, when combined with auto-configuration. NEMO provides the capability to quickly reestablish connectivity after movement of an entire network. Army users can continue to communicate with this mobile network using their original IPv6 addresses, as if they have not moved.

Inherent IPv6 features, in particular IP Security protocol (IPSec), can provide improved end-to-end security. The greater presence of IPSec should provide more security benefits to the tactical network environment, while supporting Encryption at all nodes. There are two key mechanisms within IPSec that provide enhanced security. The IP Authentication Header provides data integrity to ensure packets are coming from authenticated source. IP Encapsulation Security Payload provides data confidentiality by encrypting the payload of each IP packet.

Flow Labeling is an important facet of Quality of Service (QoS). Multimedia applications, such as teleconferencing and collaboration tools require a QoS to be usable. IPv6 supports both mandatory multicast and anycast packet distribution methods. An IPv6 message sent to a multicast address goes to each member of the set as well as allowing different scopes to be applied to multicast traffic. These multicast improvements will greatly benefit the DoD.

Anycast is a new addressing mode which causes packets to be delivered to the "nearest" node that is a member of the anycast group. This is likely to be useful for maneuvering units where bandwidth is limited and connectivity may be intermittent. It can also be useful in providing redundancy and automatic fail-over. These capabilities will contribute to overall battlefield architecture and reliability.

The advanced features of IPv6 promise many benefits for DoD, especially for the Army. Military benefits include the necessary support for future Network-centric warfare systems that will be IP-centric. These include the Army's robot and sensor-laden Future Combat System (FCS), and the DOD's Global Information Grid (GIG). All these individual features briefly described here are important to the warfighter, but the true power of IPv6 is in the architectural combination of features to drive a coherent network-centric design. Figure 3 shows the key feature comparison of IPv4 and IPv6 as well as IPv6 advantages.

IPv4 vs. IPv6
Key Features Comparison and v6 Advantages

Feature	IPv4	IPv6	Advantages
Addressing	32 bit address, 4.3B addresses	128 bit address, multiple addresses per link	Facilitates multihoming, plenty address space, scoped with lifetime
Net Mgmt	Stateful configuration	Stateless Autoconfiguration Stateful configuration (DHCPv6), router renumbering	Plug-n-fight, host renumbering simple, simplified network changes
Security	IPSec optional	IPSec mandatory, authentication & encryption	Works end-to-end @ networking layer (3)
Mobility	Add-on feature	Component feature with route optimization	Eliminates triangular routing, neighbor discovery, Autoconfig leveraged, scalable
QoS	Differentiated Service, Integrated Service	Differentiated Service, Integrated Service	Ongoing work to improve with extension headers and flow label switching
Multicast	IGMP/PIM/Multicast BGP, very limited multicast address space	MLD/PIM/Multicast BGP,Scope Identifier, vast multicast space, global unicast-prefix multicast addresses	Facilitate dissemination of information and community of interest
Header size	Variable, 20 bytes, 12 fields, checksum (non-compressible), options all included	Fixed 40 bytes, 8 fields, options in extension headers, no checksum (compressible), 64 bit alignment	Fewer fields, no checksum, faster processing, higher compression for wireless
Min Link MTU	68 byte	1280 byte (Can be smaller if size is controlled manually)	Eliminates router fragmentation
Routing	Class, hierarchical	Hierarchical	Fewer routes in core tables, less processing

Figure 3

3. IPv6 Transitioning Challenge

IPv6 technology is forging the Next Generation Internet with advanced features that synergistically contribute to a more powerful Net-centric architecture. Yet, despite many preliminary research and development efforts, there remains a substantial transitioning challenge.

The Joint Staff has established operational criteria that must be met before IPv6 can be activated on operational networks <r10>. They are:

1. Demonstrate end-to-end interoperability in a dual-stack IPv4-IPv6 environment
2. Verifies equivalent or better performance to IPv4 based networks
3. Demonstrate voice, video, and data integration
4. Demonstrate effective operation in low-bandwidth environments
5. Demonstrate scalability of IPv6 networks
6. Demonstrate security of unclassified networks operations, classified network operations, black backbone operations, integration of High Assurance IP Encryptors (HAIPE), integration of IPSec, and integration with firewalls and intrusion detection systems
7. Support mobile terminals (voice, data and video)
8. Demonstrate Transition Techniques
9. Demonstrate ability to provide NetOps of networks
10. Demonstrate small and large scale tactical deployability

The Army is expected to have the most difficult challenges among the services, because of the prevalent low bandwidth environments, large number of mobile users, ad-hoc networking, and on-the-move operational requirements. Clearly, the IPv6 transitioning process will require significant research and development analysis, robust laboratories, major testing efforts, quantifiable methods, and automated tools to satisfy these criteria.

4. Fort Monmouth IPv6 Center of Excellence

In response to the IPv6 transitioning challenge, two Army Fort Monmouth organizations, the Program Executive Office Command, Control, and Communications, Tactical (PEO C3T) Common Hardware Systems Product Directorate (PD CHS), and the Communications Electronics Research Development and Engineering Center's (CERDEC) Space and Communications Directorate (S&TCD) over two years ago formed a collaborative IPv6 team to address some of these issues.

The mission of the PD CHS office is to supply fully qualified, interoperable, and survivable tactical system hardware, and COTS software at all echelons of command for the U.S Army and other DoD services. The DoD IPv6 policy directives and risk management concerns required a prompt and pro-active organizational response from PD CHS, because it is the source of distribution to over 80 Army and DoD customers. The rationale for these initiatives was to provide value to CHS customers, avoid duplication of efforts, and attack the potential hardware issues at their source.

CERDEC S&TCD serves as the technical advisor to the Army Chief Information Officer (CIO/G6), which is charged to facilitate IPv6 transition across the entire Army. CERDEC S&TCD roles include research and development of a technically sound migration strategy and approach to guide the IPv6 transition. Once the technologies are well understood, CERDEC S&TCD is to research, evaluate and test proof of concept "use cases" for the IPv6 features and capabilities. CERDEC S&TCD meets these challenges by capitalizing on collaborative relationships with DoD component organizations such as the PD CHS, and programs such as the Small Business Innovative Research (SBIR) and the Applied Communication and Information Networking (ACIN).

Over time, and based on the success of the collaborative initiatives and IPv6 knowledge sharing, an IPv6 Center of Excellence for the entire community was established at Fort Monmouth, and new partners became engaged. Figure 4 displays the "pyramid of capabilities" now available at the Fort Monmouth IPv6 Center of Excellence.

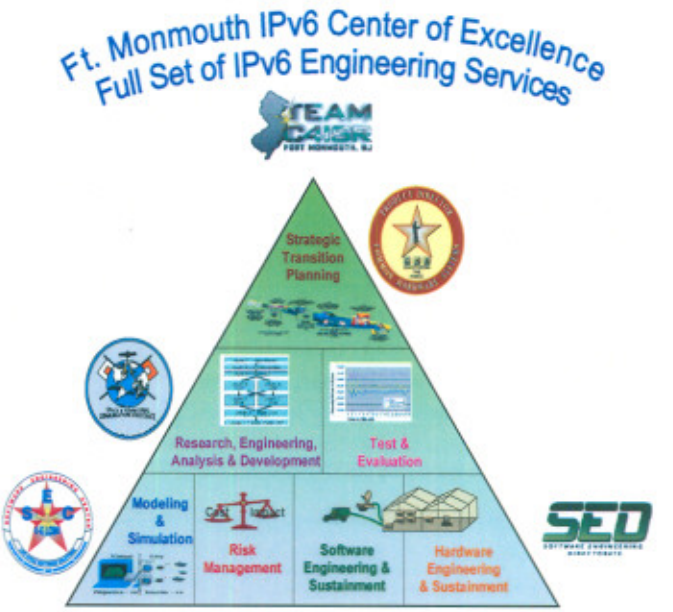


Figure 4

4.1 PEO C3T CHS & CERDEC S&TCD Laboratories

Both PD CHS and CERDEC S&TCD were early pioneers in establishing IPv6 test-beds to begin evaluating IPv6 products, and evaluate technology benefits. CHS has an IPv6/IPv4 test-bed configuration, and CERDEC has an Advanced IPv6 Research Laboratory. As collaborative IPv6 discussions began between the two organizations, the mutual benefits of linking the respective IPv6 laboratories to conduct collaborative testing became clear. Through CERDEC's link to the Defense Research Engineering Network (DREN), both organizations laboratories were connected, and could participate in the Moonv6 interoperability testing, and the Joint User Interoperability Communications Exercise (JUICE) testing. Figure 5 shows the evolving laboratory connectivity.

CHS/CERDEC Lab Connectivity
(allows for National & Joint Testing)

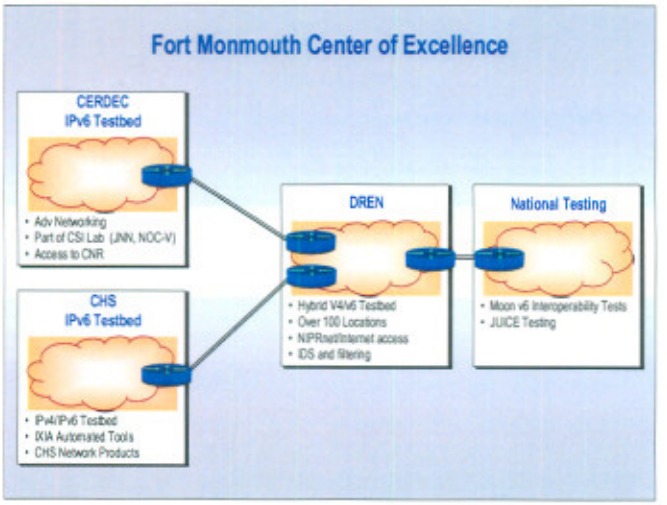


Figure 5

4.2 IPv6 Conformance Testing

One of the risk reduction activities prioritized by PD CHS was to conduct conformance testing on CHS network equipment in its IPv6/IPv4 test-bed. CHS, as an Army source equipment distributor, has a real interest in IPv6 product certification. IPv6 conformance testing should lead to product certification, and is an excellent prerequisite to interoperability testing between IPv6 and IPv4 equipment. The object is to find the problems in the laboratory, and not the field, saving time, money, and perhaps lives.

PD CHS, along with its collaborative partner CERDEC S&TCD began an effort to certify products as "IPv6 Compliant." The initial work was compliance testing on the Cisco Router model 3745 using IOS 12.3(7t) operating system for conformance to RFC 2460 from the DISR list of standards. Results from this initial effort strongly influenced the DISR IPv6 product profile. The tests were conducted in the CHS laboratory, using testing tools developed by the CERDEC S&TCD test team, and commercially available monitoring software, called Ethereal. The testing specifically focused on three IPv6 areas: the IPv6 header, extension headers and options, and fragmentation. The basic testing approach was to manipulate the fields of an IPv6 packet, send the data to a router, monitor the response sent back against an expected outcome, and save the data sent and received in a recorded file. This type of testing allowed verification of the router handling "bad packets" in conformance with RFC 2460.

The IPv6 header testing showed correct packet handling, and the assignment of appropriate error messages. The extension header tests verified the Cisco 3745 correctly processed the options and extension headers including the Hop-by-Hop options, destination options, and routing headers. Finally, fragmentation verified that the Cisco router could handle fragmented packets for both delivery and reassembly within the specified time constraints. The correct ICMPv6 error messages were sent in response to reassembly operations that exceeded the specified time constraints. This initial conformance testing provided verification that the Cisco router under test was in conformance with RFC 2460 Internet Protocol Version (IPv6) specifications, and increased confidence in defining an overall test methodology that could lead to a COTS IPv6-enabled certification process. The results were documented in a CHS/CERDEC report <r11>.

Perhaps the most important value of this testing is that it provided basic metrics for the full effort that would be entailed in conducting conformance testing against the full set of products affected by the emergence of IPv6. In addition, it also forged a test methodology to rigorously address IPv6 conformance and set the stage for follow-on interoperability testing.

The conformance testing also influenced an initial test methodology that CHS derived to validate that their products are IPv6 compliant <r12>. Tests were seen as necessary in major product categories following the convention established by the DoD IT Standards Registry (DISR). This organization lines up well with the CHS product line: routers, hosts/operating systems and firewalls. It is recognized that specific detailed test plans for each of these areas would need to be written and incorporated into the test methodology. A major tenet of the CHS approach is that IPv6 product conformance testing must occur first, before interoperability testing with IPv4 products can be conducted. Although initially most tests will require manual steps, the test methodology seeks to automate as much of the process as possible for subsequent runs against different products. A goal is therefore to create CHS reusable test library components to streamline the process, and for future use.

The work performed by the CHS and CERDEC team in both product conformance testing and methodology development had some major impacts. The conformance testing results and methodology approach was shared with the DoD IPv6 Transition Office (DITO) and DoD IPv6 Test and Evaluation Working Group (TEWG), and was recognized as having merit. DISR IPv6 Standards Technical Working Group adapted the basic approach to conformance testing, and included it in DoD IPv6 Standard Profiles for IPv6 Capable Products <r13>.

4.3 System Engineering Analysis

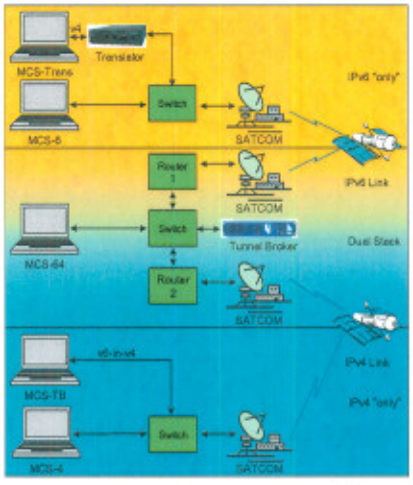
In recent years, CERDEC has conducted several engineering studies to measure and evaluate the operational functionality of IPv6 and to validate the performance and interoperability capabilities of IPv6 transition mechanisms. One such study measured the impact of the larger IPv6 protocol header, when used in the low bandwidth environment.

To examine the IPv6 performance, CERDEC constructed a modeling and simulation (M&S) environment of a Stryker Brigade Combat Team (SBCT). To conform to Future Force network requirements, the current tactical radio model of the SBCT were replaced with the Joint Tactical Radio System (JTRS) model, operating at data burst rates of 1-11 Mbps. The results indicated that when running a traffic model for the SBCT, IPv6 posed minimal impact on the overall overhead, yielding a 2-3% delta with respect to IPv4.

The savings in overhead is explained by the nature of the Time Division Multiple Access (TDMA) protocol. In TDMA networks, packets that are smaller than the allocated time slot are inefficient. As long as the "empty space" in the time slot can accommodate 20 more bytes per packet, there is virtually no difference between an IPv4 packet and an IPv6 packet traversing the tactical network.

Another significant system engineering study examined the interoperability and applicability of 17 IPv6 transition mechanisms (TM) designed to coexist or, in some cases, fully interoperate with IPv4 networks and applications. The TM evaluation considered performance, security, scalability, complexity, and cost. Based on this analysis, 5 of the 17 TMs were selected as recommended for use in Army networks. They are: Dual Stacks, manually configured tunnels, tunnel brokers, Application Layer Gateways, and translation. The next phase of the study, which included collaboration with Software Engineering Center (SEC), was to assess and demonstrate deployment scenarios and interoperability of IPv4/IPv6 dual stacks, tunneling, and the prototyping of an application layer gateway (ALG) in an environment that consists of Future Force networks, using modeling and simulation (M&S) and real Army legacy tactical networks and host equipment as shown in Figure 6.

Transition Mechanisms Interoperability Testing



Technologies Under Test:

- IPv6 Application Layer Gateway (ALG) using current force MCS
- Transport Relay Translator (TRT) using current force MCS
- IPv4/IPv6 LAP-T Translator using SBIR-developed prototype product
- Tunnel Broker using COTS product from Hexago

Benefits:

- Validate IPv6 transition technologies
- Build experience on the impact of an IPv6 transition
- Provide information sharing and education for DoD agencies

Figure 6

As it is obvious that an IPv4/IPv6 hybrid enterprise network architecture is more complex and requires more administrative overhead to configure and maintain, network designers are encouraged to employ an IPv6-dominant network that consists of an IPv6-only network core with various IPv6 transition mechanisms deployed at the edge of the network to provide interoperability.

4.4 IPv6 National and Joint Testing Efforts

The advanced networking equipment capabilities of the CHS/CERDEC IPv6 laboratories have allowed for the organizations to participate in the National Moonv6/IPv6 Capable Exercise (ICE) 2005, and the Joint Users Interoperability Communications Exercise in the summer of 2006.

Two member organizations of the Fort Monmouth IPv6 Center of Excellence, CERDEC S&TCD and PD CHS, participated in the Moonv6/ICE 2005 exercise. The focus of the testing was to evaluate the IPv6 capabilities of the Microsoft Firewall Feature Set, provided within the Microsoft Vista (beta version) operating system. The Fort Monmouth team also supported product development testing run by Spirent, Lumeta, IXIA, and SRI International. The data captured during the Moonv6 will be used to enhance vendors IPv6 products, and allow better understanding of IPv6 capabilities. A report was submitted to JITC on the Fort Monmouth participation <r14>.

The CHS/CERDEC team also participated in the JUICE 2006 exercise from the CERDEC IPv6 laboratory at Ft. Monmouth. The JUICE experiment allowed for the hands-on validation of IPv6 features for Army operational use. The demonstration was focused on two IPv6 features

that portend significant operational benefits to support the warfighter's network initialization and mobility tasks. These activities are presently manual, error prone, and time consuming tasks for highly skilled administrators. These IPv6 features were network address auto-configuration, and network mobility (NEMO) implemented with a beta IOS version from the CHS sub-contractor, Cisco Systems. The concept of this experience is shown in Figure 7. During the JUICE experience, three Army battlefield operational scenarios were employed, including a new unit joining an existing Tactical Operation Center (TOC), a unit reassigned or reorganized to join a different TOC, and a newly reassigned unit moving from the existing TOC to a different TOC. The first scenario demonstrated the benefits of auto-configuration of a router based on receiving its network prefix from the backbone. The second scenario simulated the in-theater need of creating homogenous networks from components, and the third showed NEMO (an IPv6 only feature) allowing networks to operate on-the-move with minimal user intervention.

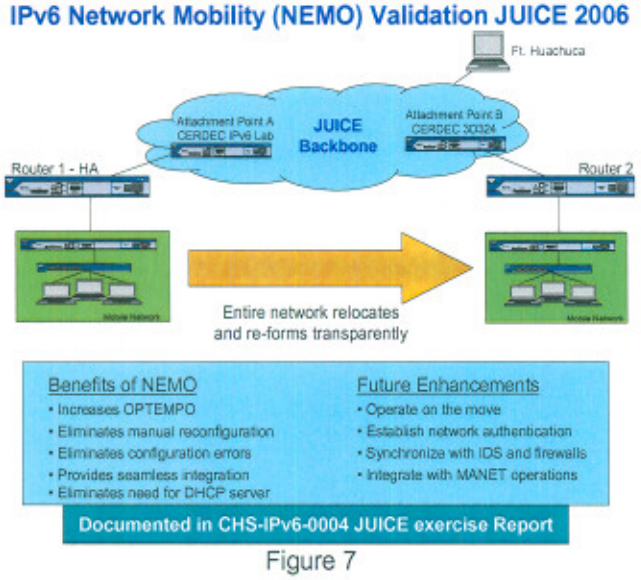


Figure 7

The JUICE experimental results verified IPv6 stateless Auto-configuration (RFC 2462), tactical reorganization capability, and Network Mobility (RFC 3963). These IPv6 features hold great promise for streamlining operations for the Army and warfighter in initializing networks, reorganizing networks, and providing network mobility. The test procedures showed compliance with IPv6 standards listed in DoD information Standards registry (DISR) and increased the confidence in CHS product quality and capabilities for IPv6. The results were fully documented in a CHS/CERDEC report <15>.

5.0 Conclusions & Future Directions

IPv6 has a wealth of advanced features and capabilities and is a critical enabler for achieving Net-centric architecture in the Army's Future Force. IPv6 has been shown, in laboratory and experimental test efforts conducted by the CERDEC/CHS team and other organizations, to be a rapidly maturing technology that promises significant operational capabilities for the warfighter. However, there are many remaining technical and deployment issues and risks that have yet to be identified, assessed, and mitigated. As the CERDEC/CHS team learned from its previous research projects, studies, testing and exercises, it is important that the Army take a holistic approach to IPv6 transition to achieve Net-centric Warfare. Capabilities documented in various RFC standards address specific functionality, but do not provide an integrated architectural solution to a system-of-systems capability for the Future Force.

The Army needs to follow a systemic risk management approach to the Future Force, developing integrated solutions that provide more powerful operational capabilities for our defense networks, platforms, and warfighters. For example, integrating the auto-configuration capability with mobile IPv6 (MIPv6) and Network Mobility (NEMO) can provide a multiplying effect, and a very powerful means for warfighters to operate continuously, while on the move, or while reorganizing, without stopping to perform manual time-consuming reconfiguration of their networks, as they detach and reattach from various network attachment points. The Army needs to continue to do the laboratory analysis, demonstration, and verification technical work, as well as to continue to perform risk mitigation on the large and complex transitioning challenges still ahead.

There are multiple courses of action for the way forward by the Army's Fort Monmouth IPv6 Center of Excellence. These courses of action can be taken in parallel to facilitate the speed of IPv6 transition.

First, continue to conduct in-depth technical analysis of the operational use of IPv6 advanced features, and their optimal transitioning mechanisms. Some pragmatic concerns are with the deployment of IPSec and its impact on existing Army Information Assurance (IA) policy, and the ability to assign multiple IPv6 addresses to a single interface. Can a unit participate in multiple communities of interest using different multicast group addresses? Can IPv6 unique feature of "flow labels" be used to support new functionalities that IPv4 can not? How should distribution methods, such as multicasting and anycasting, be used in the Future Force architecture?

Second, continue assessment of new technologies and proof of concepts, as well as new IPv6 hardware products,

through laboratory testing. Once again, the focus should be on how the advanced IPv6 features improve functional warfighting capabilities. IPv6 laboratory work and quantitative methods are absolutely essential to performance, conformance, and interoperability concerns. Security issues can also be addressed in the laboratories, such as the impact of IA devices like firewalls and intrusion detection systems (IDS), when integrated with IPSec security features.

Third, continue education and organizational outreach to share the benefits of IPv6 operational advantages from the warfighter's perspective. This will be accomplished through technical publications, professional symposiums, technology demonstrations, web based training, etc.

Fourth, welcome new organizations to the Fort Monmouth IPv6 Center of Excellence, and expand the collaborative model of laboratory linkage, technical cooperation, and information sharing.

Finally, develop and demonstrate domain "use cases," based on an integrated system of systems approach, through testing efforts like Moonv6, JUICE, and the C4ISR On-the-Move testbed. Army field exercises will also help IPv6 transitioning as a gauge to operational maturity and viability for tactical operations involving IPv6 and IPv4 network traffic. The goal of all these courses of action is to pave the way for moving IPv6 features and capabilities to the warfighter in the field.

ACKNOWLEDGMENTS

The authors would like to thank Colonel William C. Hoppe, PM TRCS and Mr. Bart Halpern, Deputy PM TRCS for their continued support of PD CHS and their IPv6 initiatives. They would like to thank Mitchell S. Mayer of the US Army CERDEC for his efforts in editing and formatting the manuscript including its graphics and charts. Finally, they would like to thank the CHS and CERDEC technical team that supported the IPv6 initiatives including Lisa Bellamy, Chris Ernst, Bob Grillo, and Joyce Kerr.

REFERENCES

<1> Alberts, David, Garstka, J.G., Stein, Frederick P., *Network Centric Warfare: Developing and Leveraging Information Superiority*, August, 1999.

<2> Committee on Armed Services submitted by Army CIO G6, *Report to Congress on Future Combat Systems (FCS) Network-Centric Status Progress*, 03 Jan 2005.

<3> *Joint Vision 2020*, United States Department of Defense, May 2000.

<4> Kuhn, Richard, Walsh, Thomas, and Fries, Steffen, *Security Considerations for Voice Over IP Systems*, NIST Special Publications 800-58, April 2004.

<5> Hagen, Sylvia, *IPv6 Essentials*, O'Reilly & Associates, Sebastopol, CA, 2002, 338pp, July 2002.

<6> Blanchet, Marc, *Migrating to IPv6*, John Wiley & Sons, Ltd, Hoboken, NJ, 2006, 418pp, 2006.

<7> Borland, David, *Army Implementation of DoD Internet Protocol Version 6 (IPv6) Mandate,* Army Deputy CIO/G-6 Memo, 5 November 2003

<8> Stenbit, John P., *Internet Protocol version 6 (IPv6)*, DoD CIO Memo, 9 Jun 2003

<9> Evans, Karen, *Memorandum issued 2 August 2005*, Office of E-Government and Information Technology.

<10> *Joint Staff Operational Criteria*, The Department of Defense Protocol Version 6, Master Test Plan, June 2006.

<11> Kerr, Joyce, *Common Hardware Systems (CHS) Equipment "IPv6 Enabled" Compliance Report RFC 2460 IPv6 Specifications applied to Cisco Model 3745 Router*, S&TCD CERDEC Report, 20 Aug, 2004.

<12> Devine, Terry and Walsh, Thomas, *PdM CHS IPv6 Test Methodology, MITRE Technical Report MTR 04W0000083*, October 2004.

<13> DISR IPv6 Standards Technical Working Group, *DoD IPv6 Standard Profiles for IPv6 Capable Products*, version 1.0, 1 June 2006.

<14> Grillo, Robert, *CERDEC/CHS Moonv6 / IPv6 Capable Exercise (ICE) 2005*, January, 2006.

<15> Kerr, Joyce, *Common Hardware Systems (CHS)/CERDEC S&TCD JUICE 2006 Exercise Report, Verification of IPv6 Stateless Auto-configuration Tactical reorganization & Network Mobility (NEMO),* 31 August 2006.